ELabELN

Administrator Manual

Team Administration and System Administration Guide

With Configuration Examples, Best Practices, and Cross-Industry Patterns

Powered by LabLynx, Inc.

www.lablynx.com | www.elabeln.com

Version 1.0 | June 2026

Table of Contents

Table of Contents 2
Preface: Who This Manual Is For 3
1. ELabELN Administration Overview 3
1.1 The Three-Tier Administration Model 3
1.2 Accessing Admin Panels 4
1.3 LabLynx Cloud vs. LabServer Deployments 4
2. Team Settings — The Admin Panel Overview 6
2.1 Admin Panel Navigation 6
2.2 The Team Tab — General Team Settings 6
Team Name and Visibility 6
Default Experiment Permissions 6
User Registration and Validation Settings 7
Onboarding Message 7
User Capabilities — What Team Members Can Do 8
3. Managing Users and User Groups 9
3.1 The Users Tab — User Account Management 9
Validating New Accounts 9
Setting Account Validity Dates 9
Adding Users Directly 9
Promoting Users to Admin 10
3.2 User Groups — Granular Permission Targeting 10
Creating a User Group 10
Using User Groups in Practice 10
4. Configuring Experiment Categories and Status Values 12
4.1 Experiment Categories 12
Creating and Configuring Categories 12
Custom ID Sequences 12
Category Planning by Lab Type 13
4.2 Experiment Status Values 13
Creating and Editing Status Values 13
Resource Status Values 14
5. Templates — Admin Configuration and Governance 15
5.1 The Admin's Role in Template Management 15
5.2 Creating Team Templates 15
Template Design Principles for Admins 15
5.3 Locking Steps — Admin Controls 16
5.4 Template Versioning Strategy 16
5.5 Resource Templates and Categories 17
6. Tag Management 18
6.1 The Tag Manager 18

6.2 Common Tag Normalization Tasks 18
6.3 Controlling Tag Creation 18
7. Bulk Export and Batch Actions 20
7.1 Bulk Export 20
Export Options 20
7.2 Batch Actions 20
7.3 Usage Reporting 21
8. Team Admin Best Practices and Workflows 22
8.1 New Team Setup Checklist 22
8.2 Ongoing Admin Routines 22
8.3 Compliance Documentation for Admins 23
9. SysAdmin Overview — The Sysconfig Panel 25
9.1 Sysconfig Panel Overview 25
9.2 First-Time SysAdmin Setup Checklist 25
10. User Account Management at the System Level 27
10.1 Creating User Accounts 27
Batch User Creation 27
10.2 Team Assignment and Multi-Team Membership 27
10.3 Role Management at the System Level 28
10.4 Access Control Audit Practices 28
11. Authentication Configuration — SSO and LDAP 30
11.1 Local Authentication 30
11.2 SAML/SSO Integration 30
What SSO Provides 30
Configuring SAML SSO — Step by Step 30
11.3 LDAP Integration 31
11.4 Multi-Factor Authentication — System-Level Enforcement 32
12. Team Configuration at the System Level 33
12.1 Creating Teams 33
12.2 Team Architecture Decisions 33
12.3 Deleting and Archiving Teams 34
13. Email, Notifications, and Timestamping Configuration 35
13.1 Email (SMTP) Configuration 35
13.2 Notification Settings 35
13.3 Timestamping Service Configuration 36
14. Security, Audit Logs, and Compliance 38
14.1 Security Settings 38
14.2 System Audit Logs 38
14.3 Backup and Recovery (sciCloud.net® Deployments) 39
Backup for LabServer (On-Premises) Deployments 39
14.4 Preparing for External Audits 39
Appendix A: Quick Reference — Admin vs. SysAdmin Capabilities 41
Appendix B: Compliance Configuration Checklist by Regulatory Framework 42

Appendix C: Troubleshooting Common Admin Issues 44

Preface: Who This Manual Is For

This manual is written for ELabELN administrators at two levels:

- Team Administrators (Admins) — users who manage a single team within an ELabELN instance. Admins configure the team's categories, templates, status values, tags, user groups, and permissions. They validate new users, view all team experiments, and run exports. This manual covers Team Admin functions in Chapters 2 through 8.
- System Administrators (SysAdmins) — users who manage the entire ELabELN instance. SysAdmins create and configure teams, manage all user accounts, configure authentication (SSO/LDAP), set security policies, and control instance-wide settings. Chapters 9 through 14 cover SysAdmin functions.

If you are a Team Admin but not a SysAdmin, Chapters 2–8 are your primary reference. If you are a SysAdmin, all chapters are relevant. Many SysAdmins also act as Team Admin for one or more teams.

This manual follows the same structure as the ELabELN User Manual: each feature is explained with what it does, why it works that way, and how different organizations use it. Cross-industry examples throughout show how the same configuration tools serve academic, pharmaceutical, forensic, clinical, and quality laboratory environments.

1. ELabELN Administration Overview

1.1 The Three-Tier Administration Model

ELabELN uses a three-tier model separating User, Team Admin, and SysAdmin responsibilities. This hierarchy ensures that each level of administration has exactly the access it needs — and no more. Understanding the boundaries of each tier is the first step to administering ELabELN effectively.

Role	Scope and Capabilities	Typical Persons
User	Creates, edits, and manages their own experiments and resources within team-defined settings. Cannot change any team or system configuration.	Researchers, analysts, students, technicians
Team Admin (Admin)	Manages everything within a single team: users, categories, templates, statuses, tags, user groups, permissions defaults, exports, and batch actions. Can view all team experiments	Lab managers, PIs, quality managers, department leads

	regardless of individual permission settings.	
System Admin (SysAdmin)	Manages the entire ELabELN instance: all teams, all users, authentication settings, security policies, email configuration, and instance-wide defaults. Inherits all Admin capabilities across all teams.	IT administrators, LabLynx support contacts, platform owners

> **Why it works this way**
> *The three-tier model prevents privilege escalation while enabling local autonomy. A Team Admin can configure everything their team needs without having access to other teams' data or system-level settings. A SysAdmin can manage the infrastructure without needing to know the scientific content of individual experiments. Each tier's capabilities are scoped to its legitimate administrative domain.*

1.2 Accessing Admin Panels

Both Admin panels are accessed from the top-right user menu after logging in:

- Team Admin Panel: Click your user avatar (top right) and select Admin Panel. This panel is visible only to users with Admin or SysAdmin role.
- SysAdmin Panel (Sysconfig): Click your user avatar and select Sysconfig. This option appears only for SysAdmin accounts.

> **Note**
> If you do not see Admin Panel or Sysconfig in your user menu, you do not have the required role. Contact your SysAdmin to request elevated access.

1.3 LabLynx Cloud vs. LabServer Deployments

ELabELN is available in two deployment models, and the scope of SysAdmin responsibilities differs between them:

Deployment Model	SysAdmin Responsibilities
sciCloud.net® (LabLynx-managed cloud)	LabLynx manages infrastructure, server maintenance, SSL certificates, software updates, database backups, and disaster recovery. Your SysAdmin manages users, teams, and application-level configuration. Infrastructure-level tasks are handled by LabLynx.
LabServer (on-premises)	Your IT team manages the physical or virtual server, operating system, Docker container orchestration, backups, and SSL. Your SysAdmin manages application configuration in addition to infrastructure. LabLynx provides technical support and guidance.

Cross-Industry Application

Most regulated organizations (pharma, forensic, clinical) use sciCloud.net® for the SOC 2 compliance, managed infrastructure, and LabLynx-handled security patching.

Organizations with strict data sovereignty requirements (government, defense, certain clinical) use LabServer to keep all data on-premises within their controlled network perimeter.

Academic institutions typically use sciCloud.net® to eliminate the IT infrastructure burden from research computing teams.

2. Team Settings — The Admin Panel Overview

The Admin Panel is the Team Admin's primary workspace. It is organized into tabs, each covering a distinct area of team management. This chapter provides a complete reference to every tab and setting.

2.1 Admin Panel Navigation

Access: Click your user avatar → Admin Panel. The panel opens in a new tab showing the following tabs across the top:

Item	Description
Team	General team settings: name, visibility, default behaviors, onboarding messages, and what users can and cannot do.
User Groups	Create and manage groups of users for granular permission targeting (e.g., QA Team, Analysts, Supervisors).
Users	View, validate, edit, and manage all users associated with your team.
Export	Bulk export experiments, resources, or booking data from your team.
Tag Manager	Edit, merge, and normalize existing tags across your team.
Batch Actions	Execute administrative actions on many entries simultaneously (e.g., change visibility, reassign ownership).

2.2 The Team Tab — General Team Settings

The Team tab contains the settings that govern your team's overall behavior. These settings affect all users in the team. The following subsections explain every significant setting group.

Team Name and Visibility

The Team Name is the display name visible to all users when they switch teams or create entries. Choose a name that is clear and unambiguous — particularly important in multi-team instances where users might belong to five or more teams.

Team Visibility controls whether the team is visible to non-members. In most cases this should be set to Private (visible only to members). Setting it to Public makes the team's name discoverable to all authenticated users on the instance, which may be appropriate for shared core facilities or institutional resource pools.

Default Experiment Permissions

This setting determines the default permission level for all new experiments created in the team. The options are:

- Only Me (Private) — New experiments are private to their creator by default. The researcher must explicitly share any experiment they want others to see. Recommended for labs with sensitive or unpublished research.
- My Team — New experiments are visible to all team members by default. The creator can restrict specific experiments to private. Recommended for collaborative labs where sharing is the norm.

- Organization — New experiments are visible to all teams in the instance. Rarely appropriate as a default; used for shared resource teams.

Why it works this way

The default permission setting shapes your team's documentation culture without removing individual control. A default of Private encourages researchers to be intentional about sharing — every shared experiment is a deliberate act. A default of Team encourages open collaboration and reduces the chance that important work is invisible to colleagues who need it. Neither is universally correct; choose based on your team's research culture and IP sensitivity.

Cross-Industry Application

Academic research lab: Default to Team for a collaborative, open culture. Students can see each other's work and learn from it.

CRO or multi-client lab: Default to Only Me. Each researcher's data is private until explicitly shared within the client project team.

Pharma QA: Default to Team so supervisors can see all in-progress QA records without needing individual sharing. Combined with read-only permission defaults, this gives visibility without edit risk.

User Registration and Validation Settings

These settings control how new users join the team:

- Allow users to self-register: When enabled, anyone who navigates to your ELabELN URL can create an account and request to join your team. When disabled, only users invited by a SysAdmin or manually added by an Admin can join.
- Require Admin validation of new accounts: When enabled, new accounts appear in a pending state and cannot log in until an Admin validates them. When disabled, accounts are active immediately upon registration (or SSO first login).

Why it works this way

Manual validation is a security control. In an open academic environment where any university email can register, validation lets the Admin confirm that the new account belongs to a genuine team member before granting access to any team data. In closed environments with SSO-only authentication, validation may not be necessary because identity is already verified by the identity provider.

Example: Validation workflow in a regulated lab

A new QA analyst joins the pharmaceutical company. HR provisions her in Active Directory. She navigates to the ELabELN instance and SSO redirects her to log in with her company credentials. Her account is created in ELabELN but appears in the Admin Panel's pending validation list. The QA Manager (Admin) sees the pending account, verifies it matches the expected new hire, validates it, and assigns her to the correct user groups. The analyst can now log in with full access to the team.

Onboarding Message

The onboarding message is displayed to users the first time they log in, or persistently as a banner at the top of all team pages (configurable). Use this to communicate team-specific guidance: naming conventions, required tags, links to your team's SOP for ELabELN use, and contact information for the Admin.

Tip

Write the onboarding message as if you are talking to someone who has just joined the team and opened ELabELN for the first time. Include: (1) your team naming convention, (2) the 3–5 most important tags to apply to every experiment, (3) which templates to use for the most common experiment types, and (4) who to contact with questions.

User Capabilities — What Team Members Can Do

A set of checkboxes controls specific capabilities for all Users in the team. Admins always retain all capabilities regardless of these settings.

Capability Setting	Effect and When to Use It
Allow users to create new tags	When enabled, any user can create new tags. When disabled, only Admins can create tags. Useful for maintaining a controlled tag vocabulary in compliance-sensitive environments.
Allow users to lock their own experiments	When enabled, users can lock their experiments independently. When disabled, only Admins can lock. Use this in environments where locking is a QA or supervisory action.
Allow users to set experiment permissions	When enabled, users control who can see/edit their experiments. When disabled, the team default permission applies to all entries — users cannot restrict or expand access themselves.
Allow users to delete experiments	When enabled, users can soft-delete their own experiments. When disabled, only Admins can delete. Suitable for regulated environments where data retention requires Admin-authorized deletion.
Show team experiments in sidebar	When enabled, the left panel shows a summary of recent team experiments for at-a-glance visibility. When disabled, the panel is hidden.
Force MFA for all team members	When enabled, MFA is required for every login by any member of this team. Users who have not enrolled are forced to enroll before accessing the team.

Cross-Industry Application

Academic lab: All capabilities enabled. Researchers have full control over their own data, can create tags freely, and can lock their own completed experiments.

Pharma GMP: Tag creation disabled (controlled vocabulary only). Lock disabled for users (locking is a QA action performed by Admin after review). Deletion disabled for users.

Forensic lab: User permissions disabled (all experiments inherit team defaults). Deletion disabled. MFA forced. These settings support the chain-of-custody and data integrity requirements of accreditation.

3. Managing Users and User Groups

3.1 The Users Tab — User Account Management

The Users tab in the Admin Panel shows all users currently associated with your team, along with their role, email, last login date, and account status. It is the primary interface for managing team membership.

Validating New Accounts

When a new user registers or logs in via SSO for the first time, their account appears in the pending list at the top of the Users tab (if validation is required per your team settings). To validate:

1. Open the Admin Panel → Users tab.
2. Review the pending account: name, email, and registration date.
3. Confirm the account belongs to a legitimate team member.
4. Click Validate to activate the account. Or click Delete if the account is invalid or belongs to another team.

> **Note**
> If a valid user has registered but appears to belong to the wrong team, contact your SysAdmin to reassign their team association rather than deleting and re-creating the account. Deleting an account removes all entries created by that user unless ownership was previously transferred.

Setting Account Validity Dates

Each user account can have a validity expiry date. After this date, the account is automatically deactivated and the user cannot log in. This is particularly useful for:

- Temporary collaborators or visiting researchers with a known departure date.
- Student accounts that should expire at the end of the academic year.
- Auditor or external reviewer accounts that should expire after the audit period.
- Contractor accounts tied to a contract end date.

> **Tip**
> Set validity dates for all non-permanent accounts at the time of creation. This eliminates the administrative effort of manually deactivating accounts when users leave, and ensures that access is automatically revoked even if HR offboarding does not trigger an IT action.

Adding Users Directly

If the SysAdmin has granted your team this capability, you can add users directly from the Users tab without requiring them to self-register. Enter the user's email address and click Add User. An invitation or password reset email is sent to the address. The new user activates their account by setting a password through the reset link.

> **Note**
> Direct user addition requires email to be configured in the SysAdmin Panel. If users do not receive the invitation email, verify with your SysAdmin that SMTP settings are configured correctly.

Promoting Users to Admin

Any user in your team can be promoted to Admin role from the Users tab. Click the user's row, locate the role selector, and change from User to Admin. The promotion takes effect immediately on the user's next page load. Demoting an Admin back to User is performed the same way.

> **Important**
>
> **Admin promotion grants significant access: the promoted user can view all team experiments regardless of permission settings, modify all team configuration, validate or delete accounts, and run batch actions on all data. Promote only users who need these capabilities for a genuine administrative reason. In regulated environments, Admin access should be documented and reviewed periodically.**

3.2 User Groups — Granular Permission Targeting

User Groups are named collections of users that can be referenced in experiment and resource permissions. Instead of sharing an entry with five named individuals, share it with the 'QA Review Team' group — all five get access, and when the group membership changes, the sharing updates automatically.

Creating a User Group

5. Open Admin Panel → User Groups tab.
6. Click Create Group. Enter a descriptive name (e.g., 'QA Reviewers', 'Analytical Chemistry', 'External Auditors 2026').
7. Type each member's name in the search box. Select from the autocomplete list.
8. Click Save. The group is immediately available in permission selectors across all experiments and resources.

> **Note**
>
> User Groups can include users from other teams on the same instance. This enables cross-team collaboration: a group called 'Joint Project Alpha' might include researchers from three different teams, all of whom can access experiments shared with the group.

Using User Groups in Practice

Group Example	How It Is Used
QA Reviewers	A group containing all QA staff. Test records are shared with this group with read access, allowing any QA member to review without being individually listed on every record.
Instrument Operators — LC-MS	A group of analysts trained on a specific instrument. The LC-MS resource (equipment record) is shared with write access only to this group, preventing untrained staff from modifying calibration records.
External Auditors	A group containing auditor accounts. All completed, signed records are shared with this group with read access during the audit window. After the audit, the group is emptied, revoking access from all auditors simultaneously.
Project Alpha Core Team	A group for a specific multi-person project. The project summary experiment and all project resources are shared with this group with

	read-write access. As people join or leave the project, only group membership needs updating.

Why it works this way

User Groups solve the permission maintenance problem at scale. Without groups, a researcher who shares an experiment with 10 named colleagues must update 10 entries every time a colleague leaves or a new one joins the project. With groups, they update one group membership and all entries sharing with that group instantly reflect the change. In organizations with high researcher turnover (academic labs, CROs, startups), this operational efficiency is substantial.

4. Configuring Experiment Categories and Status Values

Experiment Categories and Status Values are two of the most fundamental structural elements an Admin configures. Together, they define the vocabulary your team uses to classify and track experiments. They are accessed from the Admin Panel's Team tab, under the Experiments Configuration section.

4.1 Experiment Categories

Categories are administrator-defined labels that classify experiment types. Each experiment belongs to exactly one category. Categories are displayed as colored pills in the experiment index, enable one-click filtering, and support independent custom ID numbering sequences.

Creating and Configuring Categories

9. In Admin Panel → Team tab → Experiments section, click Add Category.
10. Enter the category name (e.g., 'Western Blot', 'HPLC Run', 'Case Intake').
11. Select a color for the category pill. Choose distinct colors; color-coding is a key usability benefit.
12. Enable 'Custom ID' auto-increment if you want sequential numbering within this category (e.g., WB-001, WB-002…).
13. Save. The category is immediately available to all team users.

Tip

Limit your initial category set to the 8–12 most common experiment types. Creating 50 categories at setup produces a cluttered filter panel that slows users down. Add categories as genuine needs emerge rather than trying to anticipate every possible experiment type upfront.

Custom ID Sequences

When Custom ID auto-increment is enabled for a category, ELabELN assigns the next sequential number to each new experiment in that category. Each category has its own independent counter. The prefix (e.g., 'WB-' or 'HPLC-') is appended by convention in the title, not by the system; the system assigns only the number.

Example: Custom ID design for a forensic lab

Category 'Case Intake' → Custom ID auto-increment enabled → generates 001, 002, 003...

Category 'Toxicology Analysis' → Custom ID enabled → generates 001, 002, 003... (independent from Case Intake)

Analysts title experiments: 'Case 2026-0412 — Toxicology Screen TOX-047'

The Custom ID (TOX-047 or 047) serves as the lab accession number, matching the number in the case management system. Filtering by category + Custom ID range produces all toxicology analyses within a date range.

Cross-Industry Application

Academic: Categories per technique. Custom IDs not typically used — researchers title experiments descriptively.

Pharma QA: Custom IDs enabled for CAPA, NCR, and Method Validation categories. The ID matches the QMS register number, enabling cross-system lookup.

ISO 17025: Custom IDs enabled per method category, generating a lab-internal work order number for each test.
Forensic: Custom IDs are the lab case number. Cross-referencing between ELabELN and the case management system uses this ID.

Category Planning by Lab Type

Lab Type	Suggested Categories	Design Rationale
Academic Research	Protein Biochemistry, Cell Biology, Genomics, Animal Studies, Imaging, Data Analysis, Literature Review, Protocol Design	Simple technique-based taxonomy. Students intuitively understand the categories.
Pharma QA	Release Testing, Stability, Method Validation, In-Process Control, CAPA, NCR, Equipment Qualification, Internal Audit	Compliance-driven taxonomy matching GMP record types.
Forensic Lab	Drug Chemistry, DNA/Serology, Toxicology, Trace Evidence, Digital Evidence, Firearms, QC/Proficiency	Discipline-based taxonomy matching lab section structure.
ISO 17025 Testing	Routine Analysis, Method Verification, QC Check, Proficiency Testing, Equipment Calibration, Corrective Action	Quality system–driven taxonomy for traceable test records.
Neurotechnology R&D	Fabrication, Bench Characterization, In Vitro, In Vivo/Animal, Clinical, Data Analysis, Regulatory Documentation	Project-phase taxonomy across a product development pipeline.

4.2 Experiment Status Values

Status values track where an experiment is in its lifecycle. ELabELN ships with default statuses (Running, Success, Need to be Redone, etc.), but you should customize these to match your team's actual workflow states.

Creating and Editing Status Values

14. In Admin Panel → Team tab → Experiments section, find the Status management area.
15. Click Add Status. Enter a name and select a color.
16. Optionally mark one status as the Default (automatically assigned to all new experiments).
17. Reorder statuses by dragging to reflect the natural workflow order (users see them in this order in the status selector).

Delete unused default statuses that do not apply to your lab. A status list with 12 options overwhelms users and produces inconsistent use. Aim for 5–8 clearly distinct states that represent meaningful points in your workflow.

Example: Status design for a pharma QA lab

1. In Progress (green) — default for new experiments
2. Pending QA Review (amber) — analyst complete, waiting for QA
3. QA Reviewed (blue) — QA has reviewed, awaiting supervisor approval
4. Approved (navy) — supervisor has signed and approved
5. On Hold (orange) — work paused pending external input
6. Rejected — Needs Rework (red) — QA identified issue, returned to analyst
7. Closed (grey) — record complete, locked, signed, archived

Why it works this way

Custom status values transform the experiment list from a flat archive into a workflow management tool. When a supervisor filters the index by 'Pending QA Review', they see exactly which records need their attention today. When a QC manager filters by 'Approved', they see the complete release-ready record set. The status vocabulary is the bridge between ELabELN's database and the lab's operational process.

Resource Status Values

Resources have their own independent status system, configured separately in the Resources section of the Team tab. Common resource statuses include Available, Out of Stock, Retired, Under Calibration, Quarantined, and Pending Qualification. These statuses appear in the resource index and can be used to filter resources by availability before linking them to experiments.

Tip

Add a 'Calibration Overdue' or 'Out of Service' status for equipment resources. When an instrument goes out of service, updating its status prevents researchers from creating new experiments linked to that instrument without noticing the problem.

5. Templates — Admin Configuration and Governance

Templates are the most powerful tool available to Team Admins for driving documentation consistency. This chapter covers template creation and management from the Admin perspective, including team-wide template promotion, template versioning strategy, and governance frameworks for maintaining template quality over time.

5.1 The Admin's Role in Template Management

In ELabELN, templates can be created by any user (personal templates, visible only to themselves) or by Admins (team templates, visible to all team members). The Admin's template responsibilities include:

- Creating and maintaining team templates that represent the team's documented methods and workflows.
- Reviewing and promoting user-created personal templates to team status when they represent best practices worth standardizing.
- Versioning templates when methods change, and archiving superseded versions.
- Locking critical protocol steps to enforce SOP compliance.
- Designing the metadata field structure for each template type to maximize the usefulness of the team's structured data.

5.2 Creating Team Templates

To create a team template (visible to all team members):

18. Navigate to Experiments → Templates (or Resources → Templates for resource templates).
19. Click Create. Enter a descriptive template name including the method name, version, and relevant standard where applicable (e.g., 'Western Blot — Standard Protocol v2.1').
20. Build the template: add body text structure, all required metadata fields, and steps.
21. To make the template visible to all team members (not just yourself), check the 'Make available to team' option before saving. As Admin, this option is available to you; regular users can only create personal templates.
22. Save and test the template by creating one experiment from it.

Template Design Principles for Admins

The User Manual covers general template design principles (Section 13.3). From an Admin perspective, add these governance-level considerations:

- Every template should have a designated owner: a specific person responsible for maintaining it. Template ownership ensures someone is accountable when methods change.
- Include a 'Template Version' metadata field in every team template. When you update a template, increment the version. Experiments created from older versions retain their original version number, making it traceable which version of the method was in use at any given time.
- Document in the template body text which SOP, regulatory standard, or publication the template implements. A line like 'This template implements SOP-CHEM-047 Rev. 3' creates a link between the digital record and the paper or electronic SOP system.
- Review all team templates annually. Schedule a 'Template Audit' task at the start of each year. Templates that are not used should be archived. Templates that are used but producing inconsistent data should be revised.

5.3 Locking Steps — Admin Controls

Step locking is configured in the template editor. When building a template, each step has a lock toggle. Steps where the lock is enabled become read-only in all experiments created from the template: users can check them off but cannot edit the wording, reorder them, or delete them.

The decision of which steps to lock requires judgment:

Decision	Guidance
Lock these steps	Steps derived from validated SOPs or regulatory procedures. Steps that have safety, compliance, or quality significance. Steps where deviation must be explicitly documented rather than silently skipped.
Do not lock these steps	Steps that serve as reminders or guidance but have legitimate adaptations. Steps that vary by sample type, scale, or condition. Steps added for user convenience that do not have compliance force.
Alternative: lock selectively	In procedures with mixed compliance and flexibility, lock the compliance-critical steps and leave guidance steps unlocked. Users see which steps are non-negotiable and which are flexible.

Example: Selective locking in a method validation template

LOCKED: Step 1: 'Verify instrument calibration certificate is current (due date > today)' — regulatory requirement

LOCKED: Step 2: 'Prepare primary standard per SOP-REF-012, record lot and expiry date' — GMP requirement

UNLOCKED: Step 3: 'Prepare test samples according to method specifications' — varies by sample matrix

LOCKED: Step 4: 'Document all deviations from the method in the experiment body before analysis' — QA requirement

UNLOCKED: Step 5: 'Run sequence as defined in instrument method file' — instrument-specific, may vary

LOCKED: Step 6: 'Calculate results per SOP-CALC-008 and complete result table below' — calculation procedure

LOCKED: Step 7: 'Request QA review before reporting results' — required workflow step

5.4 Template Versioning Strategy

When a method changes — due to a new SOP version, a regulatory requirement update, or an improved procedure — you must update the corresponding template. The correct approach depends on how many experiments have been created from the existing template:

Scenario	Recommended Action
Method just created, no experiments yet	Edit the existing template directly. No version conflict.
Method in use, new version is a minor correction	Create a new template with the updated content. Increment the version number in the template name. Archive the old template (remove team availability but keep it accessible for reference). Existing experiments retain the old template's structure.

Method in use, major revision or revalidation	Create a new template with a new name reflecting the major version (e.g., 'HPLC Method v1 — Legacy' becomes archived; 'HPLC Method v2 — Validated 2026' is created as the new active template). Communicate the change to all users.
SOP retired, method discontinued	Archive the template. Do not delete — existing experiments created from it must remain accessible and their template reference must be preserved.

Why it works this way

Never edit a template in place when experiments already exist from it. If you change a locked step in the active template, all future experiments will reflect the change — but existing experiments already have the previous step wording locked in. The template version history becomes inconsistent, and an auditor will rightly ask why experiments from the same template have different steps. The correct model is: old template → archive; new template → create. This preserves the complete version history of your methods.

5.5 Resource Templates and Categories

Resource templates work identically to experiment templates but apply to resource records. As Admin, you can define resource templates for each resource category (Equipment, Reagents, Cell Lines, Reference Standards, etc.) that pre-populate the metadata fields relevant to that resource type.

Resource categories are configured separately from experiment categories, in the Resources section of the Team tab. The design principles are the same: create categories that match the resource types your lab actually manages, use consistent naming, and keep the list manageable (8–15 categories is typically sufficient for most labs).

Example: Resource template for an instrument/equipment record

Template name: 'Instrument — Analytical Equipment'

Metadata fields: Instrument Name (Text), Manufacturer (Text), Model (Text), Serial Number (Text), Asset ID (Text), Location (Text), Responsible Analyst (Select from team user list), Calibration Frequency (Select: Monthly/Quarterly/Semi-Annual/Annual), Last Calibration Date (Date), Next Calibration Due (Date), Calibration Certificate Number (Text), Current Status (Select: In Service/Out of Service/Under Calibration/Retired)

Body text: Maintenance log (dates and descriptions), performance notes, known issues

Steps: Annual qualification checklist (locked): 1) Verify current calibration certificate; 2) Check for any open corrective actions; 3) Confirm user qualification records are current; 4) Update status field

6. Tag Management

Tags are user-created labels applied to experiments and resources to enable flexible, multi-dimensional organization. As users create tags freely, inconsistencies emerge over time. The Tag Manager in the Admin Panel gives you tools to clean up and normalize the tag vocabulary.

6.1 The Tag Manager

Access: Admin Panel → Tag Manager tab. The Tag Manager shows all tags in the team, the number of entries each tag is applied to, and the date each tag was last used. From this interface you can:

- Edit a tag name: Click the tag to open the edit field. Change the name and save. The tag is renamed on all entries that had the original tag — this is a rename, not a new tag.
- Delete a tag: Remove a tag and detach it from all entries. Use this for abandoned or mistaken tags with no entries, or obsolete tags after a project closes.
- Merge tags: Not a single-click operation, but achievable by renaming Tag A to Tag B's exact name, then deleting the now-duplicate.

6.2 Common Tag Normalization Tasks

Issue	Resolution
Spelling variants	'Western Blot', 'westernblot', 'WB', 'Western-Blot' all refer to the same thing. Rename all variants to the canonical form ('Western-Blot') using the edit function.
Capitalization inconsistencies	'ProjectAlpha', 'projectalpha', 'Project Alpha' should be normalized to one form. Rename all to 'ProjectAlpha' (no spaces, consistent capitalization).
Abandoned project tags	A project closed 18 months ago. Archive the experiments. Rename the tag to 'ARCHIVED-ProjectOld' to distinguish it from active project tags in the tag list.
Personally-specific tags	A user created a tag with their own initials or notebook number. If the tag is only on their own entries, it may be fine to leave. If it has been applied to shared entries, normalize to a team-standard form.
Accidental duplicates	A user pressed Enter twice and created an empty tag. Delete it.

> **Tip**
> Schedule a Tag Manager review quarterly rather than waiting until the tag list becomes unwieldy. A 30-minute quarterly review prevents the exponential growth of tag variants. Send the normalized tag vocabulary to the team after each review so users know the canonical tags to use.

6.3 Controlling Tag Creation

If your compliance or quality requirements demand a strictly controlled tag vocabulary — where only pre-approved tags may be used — disable the 'Allow users to create new tags' capability in the Team tab. With this setting disabled:

- Only Admins can create new tags.
- Users can apply existing tags to their experiments but cannot create new ones.
- The tag vocabulary is fully controlled by the Admin team.

Why it works this way

Controlled tag vocabulary is a tradeoff between flexibility and consistency. Unrestricted tag creation enables researchers to quickly capture relevant labels without administrative friction, but over time produces hundreds of near-duplicate tags that reduce search effectiveness. Restricted tag creation maintains a clean, searchable vocabulary but requires the Admin to promptly add new tags when legitimate new labels are needed. Most labs start with unrestricted creation and switch to restricted after accumulating enough data to know their stable vocabulary.

7. Bulk Export and Batch Actions

7.1 Bulk Export

The Export tab in the Admin Panel allows you to export large sets of experiments or resources in a single operation — without opening each entry individually. This is the primary tool for:

- Regulatory inspection readiness: export all records from a specific date range, category, or user before an audit.
- Project closure: export the complete experimental record for a finished project.
- User offboarding: export all experiments by a departing researcher before transferring or archiving their account.
- Compliance reporting: export structured data for periodic regulatory submissions.

Export Options

Format	Use Case
Experiments (PDF)	Generates individual PDF files for each experiment in the export set, formatted identically to the single-entry PDF export. Suitable for human-readable archiving or regulatory review packages.
Experiments (ELN archive / ZIP)	Generates a ZIP archive per experiment or a single multi-experiment archive. Each ZIP contains the experiment JSON, PDF, and all attached files. Suitable for long-term archiving and cross-system transfer.
Resources (CSV)	Exports resource metadata as a CSV spreadsheet. Useful for inventory audits, equipment register reporting, and importing into external systems.
Scheduler (CSV)	Exports all equipment bookings as a CSV file. Useful for equipment utilization reporting and audit evidence of instrument access history.
Filtered subsets	All exports can be filtered by category, status, date range, user/owner, or tag before generating. This lets you create targeted exports rather than exporting the entire team's data.

Example: Audit-ready export package for a QA lab

An ISO 17025 audit is scheduled for next week. The quality manager opens Admin Panel → Export, filters by: Category = 'Routine Analysis', Status = 'Approved', Date range = last 12 months. She selects PDF format and clicks Export. ELabELN generates a PDF for every approved routine analysis record from the past year. She downloads the package (typically a ZIP of PDFs) and saves it to the audit evidence folder. The complete analytical record — all methods, results, QC data, signatures, and timestamps — is assembled in minutes rather than days.

7.2 Batch Actions

The Batch Actions tab executes administrative operations on many entries simultaneously. These are powerful tools that affect multiple records at once; use them with care.

Action	When to Use It
Change visibility / permissions	Update the permission level of all experiments from a specific user, category, or date range simultaneously. Use after a project closes to make all project experiments read-only to non-owners.
Change ownership	Transfer all experiments from one user to another. The primary use case is user departure: move all experiments from the departing user to the PI or a successor before deactivating the account.
Change status	Update the status of many experiments simultaneously. Use at year-end to close all completed project experiments, or after a validation to mark an entire set of records as Approved.
Lock entries	Lock a set of completed experiments simultaneously instead of locking each one individually. Use at project closure or audit preparation.
Add tags	Apply a tag to a set of existing entries. Use to retroactively tag a group of experiments with a project tag, or to mark a set of records for a specific review cycle.
Archive	Move a set of experiments to archived state simultaneously. Use at project completion to clear the active index without deleting historical records.

Important

Batch Actions are irreversible in their immediate effect. There is no 'undo' for batch permission changes, batch ownership transfers, or batch locking. Before running any batch action, filter the preview list carefully to confirm it contains exactly the entries you intend to affect. Run a small test batch on 2–3 entries before executing on hundreds.

Example: Batch actions at user departure

Step 1: Export all experiments by the departing user (Export tab, filter by owner). Save the export package.

Step 2: Transfer ownership of all their experiments to the PI or team lead (Batch Actions → Change Ownership, filter by owner = departing user).

Step 3: Deactivate the user account (Users tab → set validity date to today or delete the account).

Step 4: Verify the transferred experiments are accessible to the new owner and that no entries were missed.

Result: No data loss. All experimental records are preserved under active ownership. The former user's access is revoked.

7.3 Usage Reporting

From the Admin Panel overview, Admins can generate a CSV usage report showing, per user: number of experiments created, number of resources created, number of logins, and last login date. This report supports:

- Identifying inactive accounts (users who have not logged in for 90+ days) for deactivation.
- Identifying researchers who are not using ELabELN so you can follow up with targeted training.
- Reporting ELabELN adoption metrics to management or funding bodies.
- Evidence of system use for auditors who ask whether the ELN is actively employed.

8. Team Admin Best Practices and Workflows

8.1 New Team Setup Checklist

When setting up a new ELabELN team, complete the following in order to ensure users have a well-configured environment from day one:

#	Area	Action
1	Team tab — General	Set team name, default permissions, registration/validation settings, and MFA requirement.
2	Team tab — Experiment Categories	Create 8–12 categories matching your experiment types. Assign distinct colors. Enable Custom IDs where needed.
3	Team tab — Experiment Statuses	Define 5–8 status values matching your workflow. Delete default statuses that do not apply. Set the correct default status.
4	Team tab — Resource Categories	Define resource categories. Create at least Equipment, Reagents, and Personnel categories.
5	Templates	Create team templates for your 5–10 most common experiment and resource types. Test each template by creating one entry.
6	User Groups	Create the user groups you anticipate needing (QA, Supervisors, Project Teams, External Auditors).
7	Onboarding message	Write and publish the onboarding message with naming convention, key tags, and template guidance.
8	Pilot users	Invite 2–3 pilot users and run them through a test workflow before full team rollout.
9	Full rollout	Invite all team members. Validate accounts. Run onboarding session.
10	First quarterly review	After 90 days: review tag vocabulary, update templates based on user feedback, adjust status values.

8.2 Ongoing Admin Routines

Frequency	Routine Tasks
Weekly	Review pending account validations. Check for experiments in long-standing 'Pending Review' status that may be stuck in the approval workflow. Monitor the notification feed for any system alerts.
Monthly	Review usage report: identify inactive users, follow up with non-adopters. Check for any resource records with expired calibration dates or stock levels below minimum.
Quarterly	Tag Manager review: normalize tag vocabulary, merge duplicates, archive project tags. Template audit: verify all team templates are current with active SOPs. Update template version numbers as needed.

Annually	Full user audit: review all accounts, deactivate accounts for anyone who has left the team, verify Admin accounts are still appropriate. Full template governance review. Update team onboarding message for the new year.

8.3 Compliance Documentation for Admins

In regulated environments, ELabELN administrators may need to maintain documentation of their own administrative activities. Consider maintaining an 'ELabELN Admin Log' experiment (using a dedicated template) to record:

- Template changes: when a template was updated, why, and what changed.
- Category changes: when a category was added, renamed, or archived.
- User access events: significant access grants, revocations, or role changes.
- Batch actions: what was done, to which entries, by whom, and the business reason.
- System configuration changes: any changes made at the SysAdmin level that affect the team.

Why it works this way

The ELabELN audit trail records what users do with experiments. It does not automatically document why an Admin made a configuration change. A separate Admin Log provides the rationale that auditors need: not just 'the template was changed on this date' but 'the template was changed to implement SOP Rev. 4 following validation completion'. This narrative context transforms audit trail data into a complete compliance record.

PART TWO

System Administration

Chapters 9 – 14

The chapters in Part Two are intended for SysAdmins: the person (or persons) responsible for managing the ELabELN instance as a whole. SysAdmin access is required for all settings described in this section.

9. SysAdmin Overview — The Sysconfig Panel

The Sysconfig Panel is the SysAdmin's control center for the entire ELabELN instance. It is accessed from the user menu (top right) → Sysconfig, and is visible only to users with the SysAdmin role. Every setting here affects all teams on the instance.

9.1 Sysconfig Panel Overview

The Sysconfig Panel is organized into the following tabs:

Item	Description
Users	View and manage all user accounts across all teams: create, edit, promote, demote, deactivate. The master user registry for the instance.
Teams	Create, rename, configure, and delete teams. Set team-level defaults that supplement Admin configurations.
Email	Configure the SMTP server for outgoing email: notifications, password resets, onboarding invitations. Required for most operational functions.
Security	Password policy (complexity, length, expiry), login attempt limits, MFA enforcement, and session timeout settings.
Authentication	SAML/SSO configuration for external identity provider integration (Microsoft Entra ID, Okta, Google Workspace, LDAP).
Timestamping	Configure the RFC 3161 Timestamp Authority (TSA) endpoint for all teams. Set the default TSA and configure custom TSA credentials.
API	Instance-wide API settings: enable/disable API access, configure API rate limits.
Notifications	Configure system-wide notification behavior: which events generate notifications, email notification frequency, and digest settings.
Logs	Access instance-level audit logs: all user login events, authentication events, SysAdmin configuration changes, and system errors.

9.2 First-Time SysAdmin Setup Checklist

For a new ELabELN instance, complete these SysAdmin tasks before inviting users:

#	Area	Action
1	Email (SMTP)	Configure email before anything else. Without email, users cannot reset passwords, receive notifications, or respond to Request Action events. Test by sending a test email from the panel.
2	Security policy	Set password complexity, minimum length, and session timeout. Enable MFA if required by your organization or regulatory standards. Set appropriate login attempt limits.

3	Authentication	If using SSO, configure SAML settings and test with one pilot user account before enabling for all users.
4	Create teams	Create all teams the organization needs. Assign at least one Admin to each team.
5	Timestamping	Configure the default RFC 3161 TSA. Use the default (DFN.de) for academic deployments. Use a commercial TSA (DigiCert, Sectigo, GlobalSign) for regulated industry deployments.
6	Invite SysAdmin backup	Promote at least one additional user to SysAdmin. Never have only one SysAdmin account — if that account is locked, the instance becomes unmanageable.
7	Pilot test	Log in as a regular user and verify: registration, email, SSO (if configured), experiment creation, and email notifications all work.

10. User Account Management at the System Level

The SysAdmin's Users tab in Sysconfig shows all user accounts across all teams on the instance. This is the master registry. SysAdmin-level user management capabilities extend beyond what Team Admins can do.

10.1 Creating User Accounts

Users can be created in three ways:

- Self-registration: The user navigates to the ELabELN URL, creates an account, and is either immediately active or pending validation depending on team settings.
- Admin invitation: A Team Admin adds the user directly from the Admin Panel (if the SysAdmin has enabled this capability).
- SysAdmin creation: The SysAdmin creates the account from Sysconfig → Users, specifying name, email, team, and initial role. This is the recommended approach for batch onboarding of large groups.

Batch User Creation

For large deployments (department rollout, academic cohort), the SysAdmin can import users from a CSV file rather than creating accounts individually. The CSV must include: First Name, Last Name, Email, Team (team name as configured in ELabELN). The SysAdmin uploads the CSV, previews the import, and confirms. All accounts are created and invitation emails are sent automatically.

> **Tip**
> When importing users via CSV, prepare the team and Admin accounts first. New users are assigned to teams by name — the team must exist before the import. Test with a 5-row CSV before importing 200 users.

10.2 Team Assignment and Multi-Team Membership

Each user is associated with one primary team at account creation. The SysAdmin can assign a user to additional teams from the Users tab (edit the user → add team). Users can also switch teams from their own user menu if they belong to multiple teams.

Multi-team membership is common in:

- Core facility staff: A core facility manager belongs to their own team AND to each research group team that uses the facility, enabling visibility into how groups are using the equipment.
- QA/QC personnel in pharma: QA analysts belong to the QA team AND to each production or analytical team they review, giving them cross-team experiment visibility.
- PIs with multiple groups: A PI who manages two separate research groups belongs to both teams, seeing all experiments across both without needing two accounts.

> **Why it works this way**
> *Multi-team membership eliminates the need for shared accounts or account duplication. A QA manager who needs to review experiments in five production teams does not need five accounts —*

one account with five team memberships provides the required access. Every action by that manager is attributed to a single, named identity, which is the correct model for both security and audit trail integrity.

10.3 Role Management at the System Level

The SysAdmin can promote any user to Admin or SysAdmin role from Sysconfig → Users. Role assignments are logged in the system audit log.

Action	How to Perform It
Promoting to Team Admin	From Sysconfig → Users, edit the user and change their role in the target team to Admin. Alternatively, the existing Team Admin can promote peers from the Admin Panel. The promoted user can now manage team settings, view all team experiments, and perform admin actions in that team.
Promoting to SysAdmin	From Sysconfig → Users, edit the user and check the SysAdmin box. This should be done only for users who need instance-level control. Maintain a short list of SysAdmins — typically 2–3 individuals in the IT/operations role.
Demoting an Admin	Remove Admin status from the Admin Panel (Team Admin) or Sysconfig (SysAdmin). The user immediately loses elevated access on their next page load. Their data and experiment history are unaffected.
Deactivating an account	Set the account's validity date to today or a past date, or set the account status to Inactive. The user cannot log in but their data is preserved. All experiments they created retain their attribution.

Important

Never delete a user account without first exporting and transferring ownership of their data. A deleted account removes user attribution from some system records and may break links. The correct workflow for user departure is: (1) export their data, (2) transfer ownership to a successor, (3) deactivate the account. Delete only accounts created in error that have no associated experimental data.

10.4 Access Control Audit Practices

Access control — who can access what — is a frequent focus of regulatory audits (FDA, ISO 17025, forensic accreditation). Maintain the following practices to ensure access control evidence is available:

- Review all Admin and SysAdmin accounts quarterly. Verify that each elevated account belongs to a current, active employee with a genuine administrative need.
- Log significant access changes in the Admin Log (see Section 8.3). The system records what changed; the Admin Log records why.
- When an auditor asks 'how do you control who has access?', the answer should be: every account is individually authenticated (SSO or local with MFA), role-based access is configured at team and system level, accounts are deactivated upon departure, and SysAdmin access is limited to 2–3 named IT staff.
- Generate and retain the monthly user CSV report as evidence that access was reviewed. A series of monthly reports showing consistent, appropriate user access is compelling audit evidence.

11. Authentication Configuration — SSO and LDAP

Authentication configuration is one of the most impactful SysAdmin tasks: it determines how every user proves their identity to ELabELN. ELabELN supports two authentication models, which can be used simultaneously.

11.1 Local Authentication

Local authentication is ELabELN's default: each user has an email address and password stored within ELabELN's own user database. The SysAdmin configures the password policy from Sysconfig → Security.

Setting	Recommendation and Rationale
Minimum password length	Enforce a minimum of 12 characters. NIST SP 800-63B recommends length as the primary password strength factor.
Password complexity	Require a mix of uppercase, lowercase, numbers, and special characters — or simply enforce a long minimum length (14+ characters) without complexity rules. Both approaches are acceptable under modern security frameworks.
Password expiry	Optional. NIST 800-63B actually advises against mandatory periodic password changes (which tend to produce weaker passwords as users increment a number). If your organization's policy requires periodic changes, set the interval here.
Failed login lockout	Set a limit of 5–10 consecutive failed login attempts before temporary account lockout. Lockout duration should be 15–30 minutes (not permanent, to avoid denial-of-service vulnerability).
Session timeout	Set the inactive session timeout. Shorter is more secure (15–30 minutes) but inconvenient for researchers who leave a tab open. A common balance is 60–4 hours depending on data sensitivity.

11.2 SAML/SSO Integration

Single Sign-On (SSO) via SAML 2.0 connects ELabELN to your organization's identity provider (IdP): Microsoft Entra ID (formerly Azure AD), Okta, Google Workspace, OneLogin, Shibboleth, or any SAML 2.0–compliant IdP. Users authenticate once with their organizational credentials and access ELabELN without a separate password.

What SSO Provides

- Single credential: users log in with their organizational account, not a separate ELabELN password.
- Automatic deprovisioning: when an account is disabled in the IdP (e.g., an employee is terminated), their ELabELN SSO access is immediately revoked.
- Centralized MFA: if MFA is enforced at the IdP level (which it should be), all ELabELN logins automatically benefit from MFA without additional ELabELN configuration.
- Audit alignment: login events in ELabELN correspond to authentication events in the IdP audit log, enabling correlated security investigation.

Configuring SAML SSO — Step by Step

23. In your Identity Provider, create a new SAML application for ELabELN. The application's ACS (Assertion Consumer Service) URL and Entity ID are provided by ELabELN in Sysconfig → Authentication.
24. Configure the IdP to send the following SAML attributes: email (required), first name (recommended), last name (recommended), and optionally group memberships for automated team assignment.
25. Download or copy the IdP metadata XML from your IdP admin panel.
26. In ELabELN Sysconfig → Authentication, paste the IdP metadata XML (or provide the IdP metadata URL for auto-import). Save.
27. Test with a pilot user: navigate to the ELabELN login page, click the SSO button, and authenticate. Verify the user account is created with the correct name and team assignment.
28. After successful pilot, communicate the SSO login URL to all team members and disable local password login if desired (to enforce SSO-only access).

Example: SAML configuration for Microsoft Entra ID

In Entra ID: Enterprise Applications → New Application → Create your own application → Non-gallery.

Name: 'ELabELN', set up SAML SSO. Entity ID = your ELabELN instance URL. ACS URL = your ELabELN instance URL + '/saml/acs'.

Attributes: map user.mail to 'email', user.givenname to 'firstname', user.surname to 'lastname'.

Download Federation Metadata XML from Entra ID.

In ELabELN Sysconfig → Authentication, paste the XML. Save.

Test: open a private browser window, navigate to ELabELN, click SSO. Authenticate with an Entra ID account. Verify the ELabELN user profile is created correctly.

Note

ELabELN can coexist with both SSO and local authentication simultaneously. Some users may have local accounts (legacy accounts or service accounts for API use) while others authenticate via SSO. This hybrid configuration is common during SSO migration and for machine accounts that need API key authentication.

11.3 LDAP Integration

LDAP (Lightweight Directory Access Protocol) integration connects ELabELN directly to a directory service (Active Directory, OpenLDAP, FreeIPA) for user authentication. Unlike SAML, which redirects the user to the IdP and back, LDAP authentication occurs directly: ELabELN queries the LDAP server to verify credentials.

LDAP is appropriate for on-premises deployments (LabServer) that do not have a cloud IdP configured, or for organizations that manage their identity directory on-premises and prefer direct LDAP binding over SAML federation.

Configuration Field	Description and Example
LDAP Server URL	The address of your LDAP server, including protocol and port. Example: ldap://dc01.yourlab.internal:389 or ldaps://dc01.yourlab.internal:636 (secure LDAP).
Bind DN	The distinguished name of a service account used by ELabELN to search the directory. Example: cn=elabftw-service,ou=ServiceAccounts,dc=yourlab,dc=internal
Bind Password	The password of the bind service account. Store securely; this password is stored encrypted in ELabELN's configuration.

Base DN	The starting point in the directory tree for user searches. Example: ou=Researchers,dc=yourlab,dc=internal
User filter	An LDAP filter to identify valid user accounts. Example: (objectClass=person) or (memberOf=cn=ELabELNUsers,ou=Groups,dc=yourlab,dc=internal) for group-restricted access.
Attribute mapping	Map LDAP attributes to ELabELN fields: mail → email, givenName → firstname, sn → lastname.

Tip

Use LDAPS (LDAP over TLS, port 636) rather than plain LDAP (port 389) in all production environments. Plain LDAP transmits credentials in the clear, which is unacceptable in any regulated or security-conscious environment.

11.4 Multi-Factor Authentication — System-Level Enforcement

MFA can be enabled at two levels in ELabELN:

- Team level: The Admin can require MFA for all members of a specific team (Admin Panel → Team tab → Force MFA checkbox). Users who have not enrolled are prompted to enroll on next login.
- Instance level: The SysAdmin can require MFA for all users across all teams from Sysconfig → Security. This is the highest-level enforcement and cannot be overridden by Team Admins.

When instance-level MFA is enabled, users who have not enrolled in MFA are automatically redirected to the MFA enrollment page after their next login, and cannot access any part of ELabELN until enrollment is complete.

Important

Enabling instance-level MFA enforcement will immediately lock out any user who does not have an MFA device enrolled. Before enabling, communicate the requirement to all users and provide a 2-week window for enrollment. Verify that all Admin and SysAdmin accounts have MFA enrolled BEFORE enabling instance enforcement, or you risk locking yourself out.

Cross-Industry Application

Academic: MFA optional at the team level. PIs may require it for team members handling sensitive IP or compliance-critical experiments.

Pharma regulated (21 CFR Part 11): MFA required at the instance level. All accounts must enroll before any electronic signatures are in use. This is a regulatory expectation.

Forensic/ISO 17025: MFA required at the instance level. Accreditation standards expect strong authentication controls for all analytical record systems.

Startup pre-clinical: Enable MFA early, before regulatory engagement. Retroactively enabling MFA when clinical trials begin is a disruption to users who have become habituated to logging in without it.

12. Team Configuration at the System Level

While Team Admins configure their teams from within those teams, the SysAdmin has elevated access: they can create teams, modify any team's settings, and see all teams in the instance. This chapter covers team creation, structure, and architectural decisions that affect how teams are organized.

12.1 Creating Teams

Navigate to Sysconfig → Teams → Create Team. Provide:

- Team name: the display name users will see in the team switcher.
- Team description: optional but useful in multi-team instances to explain what the team is for.
- Initial Admin: specify the user who will be the first Admin for this team. They can promote additional Admins once the team is created.

After creation, the Team Admin configures categories, templates, and statuses per Chapter 2–5 of this manual.

12.2 Team Architecture Decisions

The question of how to structure teams is often the most consequential ELabELN architecture decision an organization makes. A poor team structure is difficult to reverse — moving experiments between teams requires Admin intervention and data migration planning. Take time to design the team structure before inviting users.

Model	Structure	Best For
One team per organization (flat)	All users in one team. Simple to manage. All experiments visible to all users (depending on permission defaults).	Small to medium labs (< 20 users) with homogeneous work and no IP separation requirements.
One team per research group	Each PI's group is a team. Groups work independently with their own templates and categories. Cross-group collaboration via cross-team permissions.	Academic institutions with multiple independent research groups. Each PI is Admin of their own team.
One team per department	Each functional department (QA, R&D, Analytical, Manufacturing) is a team. Department leads are Admins.	Pharma, biotech, or industrial labs where departments have different workflows and compliance requirements.
One team per project	Projects are the team unit. Team membership changes as people join/leave projects.	CROs with multiple simultaneous clients, or project-matrix organizations. Client data separation is critical.
Hybrid: functional + project	Base teams by department, overlay project teams for cross-departmental	Large organizations with both stable functional units and dynamic cross-functional projects.

	collaboration. Users belong to their department team and their project teams.	

Example: Team architecture for a 50-person pharma company

Team 1: Analytical Development (8 analysts, 2 scientists, 1 QA) — categories for HPLC, dissolution, content uniformity, method validation

Team 2: Formulation R&D (12 formulation scientists) — categories for synthesis, screening, excipient evaluation

Team 3: Quality Assurance (4 QA staff) — categories for CAPA, NCR, audit, change control; read access to all other teams

Team 4: Clinical Supply (6 manufacturing staff) — categories for batch record, in-process control, environmental monitoring

Team 5: Regulatory Affairs (3 RA staff) — categories for submission documents, risk assessment, regulatory response

Cross-team: QA staff have read access to all teams. Senior management has a dedicated team with read access to summary experiments linked from all other teams.

12.3 Deleting and Archiving Teams

Teams that are no longer active should not be deleted — all experiments within the team would be permanently lost. Instead:

- Deactivate the team: SysAdmin can set the team to inactive, preventing new experiments from being created and removing it from users' team switcher, while preserving all data.
- Archive the team's data: Run a bulk export of all experiments and resources before deactivating. Store the archive per your organization’s data retention policy.
- Transfer ongoing work: Any experiments that are still relevant to active work should be transferred to a successor team before deactivation.

Important

Deleting a team is an irreversible action that permanently removes all experiments, resources, and user data associated with the team. This operation should never be performed on a team that has contained live research data. The only appropriate use of team deletion is removing teams created in error that have no data.

13. Email, Notifications, and Timestamping Configuration

13.1 Email (SMTP) Configuration

Email is required for ELabELN to send: password reset links, new user invitation links, experiment comment notifications, Request Action notifications, expiry alerts, and system announcements. Without correctly configured email, many ELabELN features degrade or fail silently.

Setting	Details
SMTP Server	The hostname or IP of your SMTP relay. Examples: smtp.office365.com (Microsoft 365), smtp.gmail.com (Google Workspace), smtp2go.com (third-party relay).
SMTP Port	25 (unsecured, legacy), 587 (STARTTLS, preferred), 465 (SSL/TLS, also acceptable).
From address	The email address that appears as the sender for all ELabELN emails. Use a real monitored address (e.g., elabeln@yourlab.com) not a no-reply address, so users can reply with questions.
Authentication	Most SMTP services require username and password authentication. For Microsoft 365, use an app password or OAuth2. For Google Workspace, use an app password with 2FA enabled on the account.
TLS/SSL	Always enable TLS. Sending email without encryption is inappropriate for any environment that handles research data.

> **Tip**
> Use a dedicated transactional email service (SMTP2Go, SendGrid, AWS SES, Postmark) rather than a personal or shared mailbox SMTP for production deployments. Transactional services provide delivery reporting, bounce handling, and are not rate-limited like individual user accounts.

After configuring SMTP, use the 'Send test email' button in Sysconfig → Email to verify delivery before inviting users. Common failures: incorrect port, missing TLS, authentication error, or the sending IP being blocked by a spam filter.

13.2 Notification Settings

ELabELN generates notifications for: new comments on your experiments, Request Action events sent to you, experiment status changes you follow, and system announcements from the SysAdmin. Notifications appear in the bell icon in the navigation bar and optionally as email digests.

From Sysconfig → Notifications (or individual user Settings), configure:

- Email notification frequency: immediate (each event sends an email), daily digest (one email per day summarizing all events), or disabled (in-app only).
- System announcements: Compose and send a system-wide message from Sysconfig. This appears as a notification to all users and is useful for announcing maintenance windows, major feature releases, or urgent policy changes.

> **Tip**
> Recommend that all users configure email digest notifications rather than immediate per-event email. Researchers who receive 50 ELabELN notification emails per day quickly start ignoring or unsubscribing from them, missing important Request Action events as a result. A daily digest collects all notifications into one readable summary email.

13.3 Timestamping Service Configuration

RFC 3161 timestamping requires a Timestamp Authority (TSA) endpoint. ELabELN comes pre-configured with a default TSA (DFN.de, a free academic TSA operated by the German National Research and Education Network). This is appropriate for academic deployments. For regulated industry deployments, a commercial TSA with a service level agreement is recommended.

TSA	Details	Best For
DFN.de	Free, academic community TSA. No registration required. Suitable for academic research and IP protection in non-regulated research contexts.	Academic labs, research universities, non-profit institutions
DigiCert	Commercial TSA with SLA. Free timestamping tier available. Widely accepted in regulatory and legal contexts.	Pharma, biotech, CRO, any regulated industry
Sectigo	Commercial TSA. Free service available. Well-established for legal and regulatory timestamping.	Legal, regulatory, compliance-heavy environments
GlobalSign	Commercial TSA with AATL (Adobe Approved Trust List) status. Widely accepted.	Documents, compliance, EU regulatory environments
Universign	eIDAS-qualified TSA. Required for electronic evidence admissible in EU courts and regulatory submissions under EU regulations.	European regulatory submissions, EU pharmaceutical submissions
Custom TSA	Any RFC 3161–compliant endpoint. Provide the URL and optionally authentication credentials.	Organizations with contractual TSA arrangements or private TSA infrastructure

To configure the TSA: Sysconfig → Timestamping. Enter the TSA URL (and credentials if required). Save. All future timestamp requests from any team will use this TSA.

Note

Changing the TSA does not affect existing timestamps. Timestamps already issued by the previous TSA remain valid and verifiable using their original TSA's certificate. New timestamps use the newly configured TSA. You can safely switch TSAs when a service changes or you upgrade from a free to a commercial TSA.

14. Security, Audit Logs, and Compliance

This chapter covers the SysAdmin's role in maintaining the security posture of the ELabELN instance and in providing audit evidence to internal and external reviewers.

14.1 Security Settings

Sysconfig → Security controls instance-wide security parameters. Beyond password policy and MFA (covered in Chapter 11), the key settings are:

Setting	Recommendation
Max login attempts before lockout	The number of consecutive failed password attempts before an account is temporarily locked. Set to 5–10. Too few (3 or fewer) causes frequent legitimate lockouts from typos. Too many (15+) provides inadequate brute-force protection.
Lockout duration	How long a locked account must wait before retry is permitted. 15–30 minutes is standard. Do not use permanent lockout (it requires Admin intervention to unlock and becomes a denial-of-service vector).
Session timeout (idle)	How long an authenticated session persists without activity before requiring re-authentication. 1–4 hours is a common balance between security and convenience for laboratory work.
Enforce HTTPS only	Redirect all HTTP requests to HTTPS. This should always be enabled in production deployments. HTTP transmits credentials and data in the clear.
Content Security Policy (CSP)	Restricts which external resources can be loaded by ELabELN pages. The default CSP is appropriate for most deployments; only modify if you have specific third-party integrations that require exceptions.

14.2 System Audit Logs

The system audit log in Sysconfig → Logs records events at the instance level — events that occur above or outside the scope of individual experiments:

- Authentication events: every successful login, failed login attempt, SSO authentication, and MFA verification.
- Account management events: account creation, deletion, deactivation, role changes, team assignment changes.
- SysAdmin configuration changes: any change made in the Sysconfig Panel, timestamped and attributed to the SysAdmin who made it.
- Password reset events: when a password reset is initiated and completed.
- Session events: session creation and expiry.

These system logs complement the experiment-level Changelog and Revisions (which are accessed from individual experiment records, not from Sysconfig).

Example: System log use in a security incident

A QA manager reports that an experiment record was modified at 11:45 PM on a date when the responsible analyst claims they were not working.

SysAdmin opens Sysconfig → Logs and filters by user (the analyst) and date. The log shows: no successful login by that user on the date in question.

The experiment's own Changelog shows: the modification was made by a different user who had been granted editor access to that experiment.

The SysAdmin's log search establishes that no unauthorized access occurred; the edit was by a legitimately authorized user. The question is resolved with evidence rather than assumption.

14.3 Backup and Recovery (sciCloud.net® Deployments)

For organizations on LabLynx's sciCloud.net® managed cloud, the following backup posture is maintained by LabLynx:

- Hourly database backups retained for 7 days.
- Daily complete backups retained for 30 days.
- Monthly backups retained for 12 months.
- Backups stored in a geographically distant second data center on AWS infrastructure.
- Recovery point objective (RPO): 1 hour (maximum data loss in a worst-case scenario).
- Recovery time objective (RTO): 4 hours (target restoration time after a declared disaster).

SysAdmins on sciCloud.net® do not need to configure or manage backups. If you need a point-in-time restore (e.g., to recover accidentally deleted data), contact LabLynx support with the timestamp of the desired restore point.

Backup for LabServer (On-Premises) Deployments

For on-premises LabServer deployments, the SysAdmin is responsible for backup configuration. Minimum recommended backup posture:

- Database: Automated daily backup of the MySQL/MariaDB database using mysqldump or equivalent. Retain 30+ days.
- Uploaded files: Backup the ELabELN uploads directory (where all attachment files are stored). Sync daily to an off-server location.
- Off-site copy: At least one backup copy must be stored at a geographically separate location (cloud storage, remote data center). Backups stored only on the same physical server as the application are not disaster-recovery capable.
- Recovery testing: Test the full restore procedure at least annually. A backup that has never been tested is an untested assumption, not a guarantee.

14.4 Preparing for External Audits

When an external audit (regulatory inspection, accreditation review, or client audit) is scheduled, the SysAdmin and Team Admins should prepare the following:

Audit Evidence Item	How to Prepare It

User access list	Export the current user list from Sysconfig → Users. Show auditors who has access, at what role, with what team membership. Verify all accounts are current employees with legitimate access.
Access control policy	Document the organization's process for granting and revoking ELabELN access. This should match the actual settings: self-registration policy, validation requirements, MFA enforcement.
Template inventory	Export the list of all team templates with version numbers and last modification dates. Demonstrate that templates correspond to SOPs and are version-controlled.
Audit trail evidence	For any experiment the auditor selects, demonstrate the Changelog (field-level history), the Revisions (body text history), the signature records, and any timestamps. Have a test experiment ready if the auditor wants a live demonstration.
System configuration documentation	Prepare a one-page summary of the ELabELN instance configuration: deployment model, authentication method, MFA status, backup frequency, TSA used, and hosting certifications (SOC 2 for sciCloud.net®).
Incident and change log	If your organization maintains an Admin Log (Section 8.3), produce the relevant entries. Show that configuration changes are documented and authorized.

Tip

Brief your ELabELN Team Admins before the audit on what auditors typically ask to see: how is access controlled, how are records protected from modification, how are signatures authenticated, and how is backup and recovery managed. Admins who can answer these questions fluently demonstrate system maturity to auditors.

Appendix A: Quick Reference — Admin vs. SysAdmin Capabilities

Capability	Team Admin	SysAdmin
Create / manage teams	No	Yes
Create user accounts	Limited (if enabled by SysAdmin)	Yes
Configure SSO / LDAP	No	Yes
Set password policy	No	Yes
Enforce instance-wide MFA	No	Yes
Configure SMTP email	No	Yes
Configure TSA for timestamping	No	Yes
View system audit log	No	Yes
Manage all teams' users	No	Yes
Create / manage experiment categories	Yes (own team)	Yes (all teams)
Create / manage status values	Yes (own team)	Yes (all teams)
Create / manage team templates	Yes (own team)	Yes (all teams)
Manage tags (Tag Manager)	Yes (own team)	Yes (all teams)
Create / manage user groups	Yes (own team)	Yes (all teams)
Validate new user accounts	Yes (own team)	Yes (all teams)
Promote users to Admin	Yes (within own team)	Yes (any team, any role)
View all team experiments	Yes (own team)	Yes (all teams via SysAdmin)
Run batch actions	Yes (own team)	Yes (all teams)
Export team data	Yes (own team)	Yes (all teams)
Deactivate user accounts	No	Yes
Send system announcements	No	Yes

Appendix B: Compliance Configuration Checklist by Regulatory Framework

Framework	Key ELabELN Configuration Requirements	Applicable Lab Types
21 CFR Part 11	MFA enforced (instance or team), cryptographic signatures for critical records, RFC 3161 timestamps on all approved records, session timeout 30 min or less for regulated systems, all user accounts individual (no shared logins), audit trail export available on demand.	Pharma, biotech, medical device, CRO
ISO/IEC 17025	MFA recommended, controlled tag vocabulary (disable user tag creation), all steps locked in accredited method templates, equipment records with calibration status, user access list maintained and reviewed quarterly, template versioning matches SOP version control.	Testing and calibration laboratories
ALCOA+ (general GxP)	All actions attributed to named individual accounts, SSO enforces identity, timestamps system-generated (not user-entered), raw data files attached at moment of creation, required metadata fields defined in templates, records locked after approval.	Any regulated lab: pharma, food, environmental, medical device
Forensic accreditation (ASCLD, ISO 17020)	MFA enforced, controlled permissions (users cannot set permissions), no shared accounts, experiment deletion restricted to Admins, complete audit trail for all case records, individual user access reviewed annually.	Forensic laboratories, crime labs, medical examiner offices
HIPAA	PHI not stored in experiment titles or body text (use coded identifiers), role-based access restricting PHI to authorized users only, audit log maintained and reviewable, session timeout 15–30 minutes, encryption in transit and at rest (sciCloud.net® provides this).	Clinical laboratories, clinical research, healthcare-adjacent labs

GDPR / data protection	Data residency consideration (sciCloud.net® is US-based AWS; EU-specific hosting available on request), user data export capability for subject access requests, account deletion process documented, data retention policy applied.	Organizations serving EU data subjects, European labs

Appendix C: Troubleshooting Common Admin Issues

Issue	Likely Cause and Resolution	Who Resolves It
User cannot log in	(1) Account not validated – check Users tab for pending status. (2) Account expired – check validity date. (3) Password locked – reset from Admin Panel. (4) SSO issue – verify IdP configuration with SysAdmin.	Team Admin + SysAdmin
User not receiving email notifications	(1) SMTP not configured or broken – SysAdmin tests SMTP. (2) User has email notifications disabled in their Settings – ask user to check. (3) Email going to spam – check SPF/DKIM configuration on sending domain.	SysAdmin
Template not visible to users	Template not set to 'team' visibility. As Admin, open the template, enable 'Make available to team', and save.	Team Admin
Tags growing out of control	No admin-controlled vocabulary. Consider disabling user tag creation in Team settings, then normalize the existing tags using the Tag Manager.	Team Admin
Experiment category missing from new entries	Category may have been deleted. Check the Team tab → Experiment Categories section. Re-create if deleted.	Team Admin
User cannot see team experiments	Scope is set to 'Self'. Ask user to change scope to 'Team' or 'Everything'. If problem persists, verify team membership in Users tab.	Team Admin
SSO login fails for one user	The user's IdP account attribute (usually email) does not match any ELabELN user record. Verify the email attribute in the IdP matches the user's ELabELN account email exactly.	SysAdmin
Timestamp fails	(1) TSA endpoint unreachable – check network connectivity. (2) TSA URL changed – update in Sysconfig. (3) TSA rate limit exceeded – use a different TSA or contact LabLynx.	SysAdmin
Batch action affected wrong entries	Filter was too broad. Use the Batch Actions preview step carefully before executing. Contact LabLynx support if unintended changes must be rolled back.	Team Admin + SysAdmin

ELabELN Administrator Manual

Version 1.0 | June 2026

LabLynx, Inc. | www.lablynx.com | support@lablynx.com | www.elabeln.com

ELabELN Administrator Manual is published by LabLynx, Inc. All configuration and feature details are based on ELabELN as delivered and hosted on the LabLynx sciCloud.net® platform.

© 2026 LabLynx, Inc. All rights reserved.